Journal of Information Technology (2010) 25, 109–125

palgrave-journals.com/jit/

Research article

Online social networks: why we disclose

Hanna Krasnova[1], Sarah Spiekermann[2], Ksenia Koroleva[1], Thomas Hildebrand[3]

[1]Institute of Information Systems, Humboldt-Universität zu Berlin, Berlin, Germany;
[2]Institute for Management Information Systems, Vienna University of Economics and Business, Vienna, Austria;
[3]European School of Management and Technology, Berlin, Germany

Correspondence:
H Krasnova, Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Straße 1, Berlin 10178, Germany.
Tel: +49 (0)30 2093 – 1607;
Fax: +49 (0)30 2093 – 5741;
E-mail: krasnovh@wiwi.hu-berlin.de

Abstract

On online social networks such as Facebook, massive self-disclosure by users has attracted the attention of industry players and policymakers worldwide. Despite the impressive scope of this phenomenon, very little is understood about what motivates users to disclose personal information. Integrating focus group results into a theoretical privacy calculus framework, we develop and empirically test a Structural Equation Model of self-disclosure with 259 subjects. We find that users are primarily motivated to disclose information because of the convenience of maintaining and developing relationships and platform enjoyment. Countervailing these benefits, privacy risks represent a critical barrier to information disclosure. However, users' perception of risk can be mitigated by their trust in the network provider and availability of control options. Based on these findings, we offer recommendations for network providers.
Journal of Information Technology (2010) **25,** 109–125. doi:10.1057/jit.2010.6
Keywords: online social networks; online communities; motivation; privacy; information disclosure; structural equation modeling

Introduction

Online social networks (OSNs) are a relatively young but rapidly growing phenomenon on the Web. They stand for online environments where people can present themselves on their individual profiles, make links to other users and communicate with them (Gross and Acquisti, 2005). Even though a variety of web services can be described by this definition, in this study we concentrate on platforms such as Facebook or the German StudiVZ where connecting and sharing information with existing friends is the main goal.

With their rising user base, OSNs are currently among the most popular websites on the Net. Facebook alone has around 300 million active users (Facebook.com, 2009). However, the growing popularity of OSNs has been overshadowed by the privacy problems they pose. Because of the richness of the personal information users provide, OSNs cannot escape the critical eyes of privacy rights activists and scholars.

Various parties may benefit from users who publish personal information on OSNs. The voluntarily up-dated and highly identifiable user profiles offer unprecedented opportunities for customer segmentation, data mining, micro-segmented online advertising and direct communication. Commercial agents such as marketers or insurance companies can collect, store and process available OSN user data. In the working world, HR-Management can use online information to gain insights into the psychology of potential or current employees. Beyond third parties, the OSN providers themselves are naturally interested in capitalizing on their unique user-provided content. In fact, anecdotal evidence suggests that the commercial valuation of OSNs is based on active user participation rather than actual financial performance (Krasnova *et al*., 2008). Finally, published information can be abused by online crooks, stalkers and bullies – or even one's own friends (Hogben, 2007).

Despite these existing threats, people continue to reveal massive amounts of personal information on OSNs. As Acquisti and Gross (2006: 1) put it: 'one cannot help but marvel at the nature, amount, and detail of the personal information some users provide.' The question is: given the obvious potential for abuse, aren't users concerned about their privacy? Aren't there any privacy mechanisms that could regulate some of the observed self-disclosure behavior? What concrete benefits so powerfully motivate users to engage in this process? And by what costs are they offset? To investigate these questions, this study empirically examines the motivating and discouraging factors for information disclosure on OSN platforms.

This paper is organized as follows. First, we analyze the literature on motivation for self-disclosure and identify factors that may apply to the OSN context. Recognizing the unique character of OSNs, we confirm and compliment our theoretical framework with behavioral factors observed during two focus groups (FGs) with OSN users. On this basis, we formulate and empirically test an information disclosure model for the OSNs. In line with Privacy Calculus theory (Dinev and Hart, 2006), our model assesses the trade-offs OSN users make between the perceived risks and benefits of self-disclosure. Looking at the dynamics of these trade-offs, we then suggest guidelines for how today's OSN providers may ensure future growth and network sustainability.

Information disclosure on OSNs: a theoretical background

Self-disclosure is traditionally defined as 'any message about the self that a person communicates to another' (Wheeless and Grotz, 1976: 47). Apart from providing personally identifiable information, OSN users reveal other private information such as hobbies, tastes in music, books, movies, relationship status and sexual preferences on their profiles (Gross and Acquisti, 2005). Furthermore, it is common to upload one's photos and communicate news on the Wall or by posting comments.

The theoretical foundations of self-disclosure go back to Social Exchange theory, which posits that interpersonal relationships are based on a subjective evaluation of benefits and costs (Homans, 1958). This logic has formed the basis for Privacy Calculus theory, which argues that some users feel that the returns for disclosure offset the risk of their privacy being compromised (Culnan and Armstrong, 1999; Dinev and Hart, 2006). In this sense, privacy loss is seen as the price of acquiring desired benefits (Hui *et al*., 2006).

Addressing the benefits side in an interpersonal setting, Joinson and Paine (2007) argue that the benefits of a relationship, such as trust building, mutual empathy and reciprocation, often outweigh the costs associated with increased vulnerability. In the context of E-commerce, Hui *et al*. (2006) find that online companies can induce user self-disclosures – expressed mainly by revealed personal preferences, financial figures and contact details – by offering them extrinsic (e.g. time savings, self-enhancement) and intrinsic (e.g. pleasure) benefits. Although no study to date has systematically studied the benefits of self-disclosure on OSNs, initial insights suggest that enjoyment (Rosen and Sherman, 2006; Sledgianowski and Kulviwat, 2008), self-presentation (Boyd, 2007) and the ability to maintain social ties (Ellison *et al*., 2007) may all contribute to user participation and self-disclosure.

In the context of E-commerce, users' willingness to participate in an online transaction is shown to be negatively related to their perception of privacy risks (e.g. McKnight *et al*., 2002b; Pavlou, 2003; Malhotra *et al*., 2004); OSN-related literature, however, has yet to determine the exact relationship between privacy risks and actual self-disclosure. On the one hand, Krasnova *et al*. (2009) find a significant link between privacy concerns and self-disclosure, suggesting that users do account for privacy risks when they decide to self-disclose. On the other hand, Acquisti and Gross (2006) find a discrepancy between claimed privacy concerns and disclosure behavior on OSN sites. The authors suggest that this discrepancy can be partially explained by the fact that users trust OSN providers and network members and rely on their ability to control access to personal information. Studies conducted in the context of E-commerce (Pavlou, 2003) and online communities (Ridings *et al*., 2002) stress the role of trust in alleviating privacy risks. In the context of OSNs, Dwyer *et al*. (2007) develop a conceptual model of information sharing that integrates both trust in the OSN provider and trust in OSN members, viewing them as factors that countervail Internet privacy concerns. Empirical evaluation of their model, however, provides little insight into the relationship between trusting beliefs and resulting behavior. Underscoring the role of control, Culnan and Armstrong (1999) argue that letting consumers be in charge of their information is a pre-condition to mitigate privacy risks and improve trust. Xu *et al*. (2008) provide evidence for this rationale in the context of OSNs, showing that control perceptions influence the formation of individual privacy concerns.

Overall, theoretical literature provides a number of important insights into the factors behind individual self-disclosure. In particular, we find that perceived benefits, perceptions of control, and beliefs relating to risk and trust have been applied in a variety of contexts as the integral elements of the privacy calculus framework. However, despite many similarities to the already investigated settings, OSNs represent environments with significantly distinctive characteristics, which may prove relevant to user self-disclosure (Xu *et al*., 2008). For example, lack of anonymity, public availability of personal information, and interplay between online and offline communication contexts may all influence the way OSN users disclose personal information. To date, findings explicitly related to disclosure dynamics on OSNs remain limited and are mostly of a qualitative nature (e.g. Acquisti and Gross, 2006; Stutzman, 2006; Boyd, 2007; Strater and Richter, 2007). Aiming to fill this gap, we adopt a two-stage approach. In the first step, we use a content analysis of two FGs to confirm and compliment our theoretical findings. In the second step, we integrate our qualitative and theoretical findings into a model of self-disclosure on OSNs, which we then evaluate empirically.

Qualitative research on self-disclosure behavior on OSNs

Set-up of Focus Groups

Because few studies have systematically addressed self-disclosure dynamics on OSNs, FGs were conducted in winter 2008 to uncover the particularities of self-disclosure behavior on OSNs. A total of 16 students under 30 of mixed gender (nine female and seven male), from different cultural backgrounds (31% German and 69% international), and active on OSNs were invited to a 2-h discussion at the Humboldt-Universität zu Berlin in Berlin, Germany. Invited participants were evenly split between two independent sessions. We included multiple cultural backgrounds since many OSNs benefit from their international reach. Thus, around 70% of Facebook members come from outside the USA (Facebook.com, 2009). Both FGs were guided by a structured set of open questions on disclosure

motives and concerns. FG participants were intentionally not prompted regarding specific factors that motivated or discouraged their self-disclosure behavior, but rather asked to provide their opinions on questions like: 'Why do people reveal information on OSNs? Do you have any concerns when you are on an OSN?' The discussions were transcribed, resulting in a 27,404-word document that served as the basis for our content analysis.

Following the methodological guidelines of Ryan and Bernard (2000), we derived a preliminary set of themes, relating to self-disclosure dynamics, on the basis of the theoretical insights described above. Additional themes and sub-themes were induced from the FG transcripts, resulting in 15 codebook categories. In the next step, two independent coders assigned 298 total keywords from the transcripts to the identified categories of our coding scheme. A total of 259 keywords were assigned to the same categories by both coders (see Table 1, column 'Frequency').

Inter-coder reliability was 0.840 (P-value $<$ 0.000), suggesting a high level of agreement between the coders (Landis and Koch, 1977). Table 1 gives an overview of the identified categories along with their codebook definitions, the frequency with which they were mentioned (only keywords where both coders agreed were counted) and the relative importance of each category. The relative importance can be interpreted as the weight participants assign to a particular theme.

Results of Focus Groups

In line with our theoretical findings, OSN users seem to see both benefits and costs associated with their self-disclosure, as well as several factors that mitigate the costs. On the benefits side, the *Convenience of Relationship Maintenance* was by far the most important factor leading users to share information through the OSN platform: 'Social Networks allow [me] to easily maintain a tiny contact to everyone' was a typical remark of FG participants. This motive was closely followed by the *Enjoyment* obtained by using the platform, the desire to *Build new Relationships* and *Self-presentation*.

On the cost side, *Perceived Privacy Risks* were a key factor discouraging users from disclosing information. In addition to typical privacy threats observable on E-commerce sites, participants mentioned their concern about specific OSN risks such as secret sharing, bullying or profile viewing by third parties (e.g. employers). Yet, participants also argued that existing risks could be mitigated by the ability to *Control* personal information (i.e. through privacy settings or a privacy policy. Equally, *Trust in OSN Members* and the *OSN Provider* were mentioned as a way to alleviate their perceptions of risk. Existence of privacy laws (*Legal Assurance*) regulating the use of personal information was barely mentioned and, hence, was excluded from the further analysis.

One noteworthy finding of the qualitative study is that participants engage in a conscious 'privacy calculus' when cognitively deciding whether or not to self-disclose. More than once, FG participants explained that they would carefully control and limit their personal disclosure (*Information Disclosure*) in both amount (breadth) and content (depth) as a response to perceived privacy risks: 'I do not put a lot of information on the Web' or 'I try not to reveal such information which can backbite on me later.' although FG participants seem to be aware of privacy risks, they admit to disclosing information to gain certain benefits; this involves a dynamic that may not be readily observable from the outside: 'I reveal, for example, … the things which I would like at least an average person to know about me, not details … like political views, it is very important for me … because I'd like to discuss these things and I'd like people to know that I am with such views … but personal information … just status, but nothing more … and hobbies ….'

At the same time, 'classical' privacy-related behavior strategies used on the Web, such as *Information Falsification* (Son and Kim, 2008), seemed to be of little relevance. Other non-informational varieties of privacy behavior, such as the use of *Privacy Settings*, *Selectivity in Friends* and *Complaining*, were also barely mentioned by FG participants. Thus, these strategies were not included into the further analysis.

In summary, it is important to note that the findings from our FGs confirm and compliment the theoretical framework described above. Above all, they help us get an in-depth understanding of the benefits motivating OSN self-disclosure. Our qualitative findings are embedded in the model of self-disclosure and discussed extensively in the next section, where the hypotheses are formulated.

Towards a model of self-disclosure on OSNs

Self-disclosure on OSNs can take the form of self-communication on a user's profile and in the process of communication with others (e.g. by posting comments, participating in group discussions, posting on the Wall). Self-disclosure is typically measured in terms of the breadth and depth of the revelations a user makes (e.g. Metzger, 2004). Breadth reflects the amount of disclosed information, which is a function of the frequency and duration of the disclosures (Wheeless and Grotz, 1976). On the other hand, depth reflects the degree of intimacy and is also a function of the user's honesty, accuracy and intent (Wheeless and Grotz, 1976).

In this article, we consciously focus only on the *breadth* dimension of self-disclosure. We do so for several reasons. First, the economic value of a platform is *not* defined by how intimate users' revelations are, but rather by their participation, interaction and willingness to present themselves on the platform (Krasnova *et al*., 2008). Second, depth is a highly subjective variable. Evaluation of message depth requires understanding of the perception of disclosure by others, which is highly dependent on a given situation. Indeed, the interpretation and thereby the sensitivity of *any* – even seemingly harmless – piece of information depends upon the context (Joinson and Paine, 2007); this context is something that we cannot judge. Moreover, the longevity of the information released online accentuates contextual factors and increases the importance of understanding the dynamics behind the breadth of self-disclosure.

By building on the above literature review and integrating insights from the FGs, we can formulate a model of self-disclosure behavior on OSNs. In line with privacy

Table 1 Results of the focus group coding procedure

Category name	*Category definition*	*Frequency*	*Relative importance (%)*
Benefits of disclosure			
Convenience of maintaining relationships	The value users derive from being able to efficiently and easily stay in touch with each other on OSNs	46	17.8
Enjoyment	The value users derive from having pleasant and enjoyable experiences on OSNs	10	3.9
Relationship building	The value users derive from being able to build up new connections to others on OSNs	9	3.5
Self-presentation	The value users derive from being able to improve their self-concept in relation to others using OSNs (analogue to Hui *et al*., 2006)	7	2.7
Cost of disclosure			
Perceived privacy risk	Beliefs about the potential uncertain negative consequences related to individual self-disclosure on OSNs (analogue to Kim *et al*., 2008)	97	37.5
Cost mitigating factors			
Control:			
• Platform-enabled	Beliefs about one's ability to prevent undesired events on OSNs using privacy control options and privacy policies (analogue to Skinner, 1996)	18	6.9
• Legal assurance	Beliefs that legal structures like regulations, laws or other procedures adequately protect user privacy	5	1.9
Trust in OSN members	Beliefs that OSN members possess characteristics that inhibit them from engaging in opportunistic behavior (analogue to McKnight *et al*., 2002a)	17	6.6
Trust in OSN provider	Beliefs that the OSN provider possesses characteristics that inhibit it from engaging in opportunistic behavior (analogue to McKnight *et al*., 2002a)	8	3.1
Privacy-related behavior			
Information disclosure	Extent of information a user provides in the process of participation on an OSN (e.g. on the profile, in the process of communication with others)	29	11.2
Information falsification	Intentional provision of dishonest or inaccurate information on OSNs	1	0.4
Selectivity in friends	Extent of selectiveness when accepting friendship requests from others or inviting others to join one's contact list	6	2.3
Privacy settings	Extent of reliance on privacy settings	5	1.9
Complaining	Notification of OSN provider or other parties regarding inappropriate behavior of others	1	0.4

calculus theory, we systematically distinguish between two independent explanatory paths for self-disclosure: (1) 'perceived benefits' and (2) 'perceived privacy risks.' These two dimensions involved in the cognitive decision to disclose personal information, and the factors that influence them, will be derived in the following paragraphs.

Perceived benefits of information disclosure on OSNs

Convenience of maintaining relationships

The most important benefit identified in the FG sessions was the ability to conveniently maintain relationships; OSNs offer users the opportunity to efficiently communicate with each other, as all friends are 'just one click away' (FG quotation). In addition, OSNs provide users with enhanced possibilities for reciprocation – a factor critical to the maintenance of close social relationships (Homans, 1958) – without the need to invest too much time or effort: 'For me the biggest value lies in being connected to people, you just have them in your friends' list and can send them a quick message, remind [them] about yourself' (FG quotation). Furthermore, compared to traditional communication tools such as email or instant messaging, OSNs allow users to conveniently and informally broadcast news and updates to a large group of friends: 'If you have like 500 friends, it takes you time to write e-mails to every one; but on Facebook you can just write "hey, what's up?" It's easy, because you don't feel like you have to write a long e-mail…' (FG quotation).

Hui *et al*. (2006) argue that time savings, a typical outcome of convenience, can motivate consumers to disclose personal information. Hann *et al*. (2007) support this hypothesis by showing that users are ready to give up some of their privacy to gain more convenience through personalization or decreased frictional costs. Thus, aiming to maximize their utility, consumers try to minimize the time input necessary to carry out a transaction. Following this rationale, the ease of relationship maintenance and related expectations regarding networking value may motivate users to choose OSNs as their main communication medium and share their information there regardless of existing privacy risks. We therefore hypothesize:

Hypothesis H1a: Users' beliefs regarding a network's ability to aid them in conveniently maintaining relationships are positively related to their self-disclosure on OSNs.

Relationship building

Despite the common notion that OSNs manage existing networks of people who know each other from the physical world, our FGs show that users are also motivated to use OSNs to build and support new relationships. By being connected to a wider range of people, users are given the opportunity to accumulate social capital as new contacts may provide them with useful information or perspectives (Ellison *et al*., 2007). Ellison *et al*. (2007) find that intensity of Facebook usage is positively related to the creation of such weak ties.

According to interpersonal theories, an intention to develop new friendships is often tightly connected to information disclosure (Gibbs *et al*., 2006). When a user discloses more information, that user sends desired signals to others which help her to initiate contact with them (Lampe *et al*., 2007). As one participant in the FG put it: 'I provide information so that people, who share my hobbies, are able to contact me.' We therefore hypothesize:

Hypothesis H1b: Users' beliefs regarding relationship-building opportunities on OSNs are positively related to their self-disclosure on these networks.

Self-presentation

Boyd (2007: 11) views self-presentation as a central element of OSN participation: 'Through profiles, teens can express salient aspects of their identity for others to see and interpret.' On OSNs, asynchronous forms of communication are conducive to impression management, as participants have the time to formulate the impression they wish to produce (Walther, 1996): 'the image that I want to put about myself on Facebook is like my image in the mirror. I have to think what I want to reveal' (FG quotation). Furthermore, stress on verbal as opposed to nonverbal communication cues gives users the opportunity to present only desirable information about themselves – a control possibility they may not possess in real-world face-to-face encounters (Ellison *et al*., 2006): 'I reveal information which I am proud about' (FG quotation). Driven by the desire to self-present, OSN members make use of the available functionality by expanding on their achievements and experiences on their Wall, sharing photos and taking part in groups they deem appealing. OSN-related empirical studies confirm that self-presentation benefits positively influence platform participation (e.g. Krasnova *et al*., 2008). We therefore hypothesize:

Hypothesis H1c: Users' beliefs regarding self-presentation benefits are positively related to their self-disclosure on an OSN.

Enjoyment

Muniz and O'Guinn (2001) show that customers enjoy conversations in Internet communities. Similarly, Hui *et al*. (2006) recognize that service providers can exploit pleasure motives to induce users to reveal personal information. Rosen and Sherman (2006) view OSNs as purely hedonic platforms, arguing that enjoyment is a more powerful predictor of participation than perceived usefulness: 'for me it is just entertaining' (FG quotation). In fact, OSN platforms use many affect-driving features to encourage users to participate and reveal more personal details. Examples are applications such as 'iLike' or 'Compare Tastes' on Facebook, which induce users to reveal their preferences regarding movies, music, books, etc. Since users enjoy such applications, it should be no surprise that 'more than 70% of Facebook users engage with Platform applications' every month (Facebook.com, 2009). The importance of Enjoyment benefits for OSN participation and self-disclosure is also supported by empirical findings by Krasnova *et al*. (2009) and Sledgianowski and Kulviwat (2008). Therefore, we hypothesize:

Hypothesis H1d: Users' enjoyment of platform use is positively related to their self-disclosure behavior on OSNs.

Perceived cost of information disclosure on OSNs

Empirical research uses perceived privacy risks and/or privacy concerns to reflect the cost dimension of the privacy calculus equation. Both constructs are risk-related beliefs (Dinev and Hart, 2006) that negatively affect user participation (e.g. McKnight *et al*., 2002b; Dinev and Hart, 2006). However, Malhotra *et al*. (2004) argue that privacy concerns reflect a personal pre-disposition to worry about privacy, and are therefore antecedent to risk beliefs, which are defined as the expectation of losses related to self-disclosure. Following this conceptualization, we integrate the Perceived Privacy Risk construct as an impediment to self-disclosure in our study.

Beyond privacy risks typically mentioned in the E-commerce context, such as the collection and secondary use of information by service providers (Malhotra *et al*., 2004), OSNs involve particular risks associated with the public accessibility of users' information: secret sharing, collection and sharing of information by third parties, identity theft or use of the information for phishing (Hogben, 2007). As one FG participant noticed: 'I am afraid my information can land in bad hands.'

Surveying prominent media coverage of OSNs, Rizk *et al*. (2009) identify main controversies that have surrounded the issue. These include the use of information for personalized advertising, availability of private information to others via Beacon application and the sharing of personal data. Escalated media coverage, combined with negative personal experience, inevitably influences user perceptions of privacy threats (Wieschowski, 2007). This awareness of daunting privacy risks is likely to diminish a user's disposition to share information on OSNs: 'Last week I deleted all my photo albums from StudiVZ, because I saw that a lot of people are visiting my profile and I thought what the hell they are looking in my private photos' (FG quotation). Thus, we hypothesize:

Hypothesis H2: Users' perceived privacy risk is negatively related to their self-disclosure behavior on OSNs.

Cost-mitigating factors

Trust in the OSN provider and in OSN members

The construct of trust is multidimensional and context-dependent (Mayer *et al*., 1995). Addressing researchers of Information Systems, Gefen *et al*. (2003) argue that it is important to distinguish between *trust as a belief* in the beneficial qualities of the other party and *trust as an intention* to assume risk and make oneself vulnerable to others (Mayer *et al*., 1995; Chopra and Wallace, 2003). In line with Dinev and Hart (2006), in our study we define trust as truster's *beliefs* that the other party possesses characteristics that inhibit it from engaging in opportunistic behavior (McKnight *et al*., 2002a, b). Recognizing that there are many ways to classify trusting beliefs, we differentiate between three distinct categories: *competence* (trustee's ability to do what is needed by the truster), *benevolence* (trustee's caring about and acting in the best interest of the truster) and *integrity* (trustee's honesty and commitment-keeping) (McKnight *et al*., 2002a).

Studies concentrating on E-commerce find that trusting beliefs can positively impact the willingness to participate in the transaction by mitigating the magnitude of risk perceptions (e.g. Jarvenpaa and Tractinsky, 1999). According to Social Exchange theory, trust can be seen as a way to reduce the perceived costs of social transactions and encourage users to participate in them (Metzger, 2004). Although the literature does not have a uniform answer on the relationship between trust, risk and resulting behavior, Gefen *et al*. (2003) mention that, in situations where risk is inherent to an activity, trust will serve as a risk-reducing strategy; risk, in turn, will directly impact behavior. Kim *et al*. (2008) support this claim, arguing that the importance of trust increases in situations where engaging in an activity is perceived as risky and an individual does not have full control over the outcome. We believe that this is also the case for OSNs, as there are a large number of potential privacy threats resulting from individual self-disclosure (Hogben, 2007). We therefore assume that, in the context of our study, the following hierarchy of effects takes place: trusting beliefs mitigate risk perceptions, which then impact self-disclosure behavior.

Many authors make a distinction between *trust in the E-commerce vendor* and *trust in online interpersonal interactions* (e.g. Chopra and Wallace, 2003; Feng *et al*., 2004). In line with Dwyer *et al*. (2007), we argue that this distinction is critical in the context of our study, as users have to equally trust that OSN provider and OSN members will not misuse information available to them through the platform. Building on the interpersonal model of trust (Chopra and Wallace, 2003), we therefore differentiate between trusting beliefs about the OSN provider and trusting beliefs about OSN members.

Trust in OSN provider

Even though FG participants admitted that they were vulnerable to the OSN provider, they claimed to trust that it would not misuse their information: 'I have enough trust in Facebook and how they manage my data.' Their trusting beliefs were partly based on the calculative reasoning: 'if it spreads out that they are using our information, people will start to migrate to other networks' (FG quotation).

McKnight *et al*. (2002a) argue that, in situations where users choose to disclose their personal information to the service provider, they will be more concerned about its benevolence and integrity and less about its competence. In our study, we do not include the assessment of the OSN provider's competence in our trust conceptualization, but instead concentrate exclusively on beliefs about the provider's benevolence and integrity. We argue that if an OSN provider is perceived to be caring, honest and consistent in its dealings with users, participants may feel little risk in providing their personal information on the platform. We hypothesize:

Hypothesis H3a: Users' trust in the OSN provider reduces their perceived privacy risk of disclosing on an OSN.

Trust in other OSN members

FG participants singled out OSN members as another threat to their privacy: 'I am more scared about what other people

comment on or when they tag me in pictures.' Obviously, any user can engage in privacy violations – independent of whether or not she belongs to the contact list of a potential privacy victim. However, the mere fact of being friends on an OSN may serve as an indicator of a higher level of trust attributed to this person as opposed to all others not in the contact list: 'I would not trust people whom I do not know and usually I do not make friends with them [on Facebook]' (FG quotation). In line with these insights and in an attempt to reduce the model complexity, in this study we concentrate exclusively on OSN members who do not belong to the user contact list.

Generally, uncertainty about negative outcomes resulting from the actions of other OSN users can be magnified by the lack of face-to-face contact and visual cues (Ridings *et al*., 2002). Since users are unable to monitor other members on the network, they have to implicitly trust them not to abuse their personal information. Perceived similarity between other members and oneself as well as the sense of virtual intimacy produced on the platform can, however, provide a basis for the development of trusting beliefs (Walczuch and Lundgren, 2004). Users may idealize their audience and hence attribute less risk to their self-disclosures. Therefore, individual beliefs about the trustworthiness of other OSN users may mitigate privacy-related fears.

In the context of inter-personal relationships, the competence dimension of trusting beliefs typically reflects one's ability to converse on a particular topic (Ridings *et al*., 2002). OSNs, however, do not center on a specific subject. As a result, we do not include the assessment of the competence beliefs in our construct operationalization, instead concentrating exclusively on beliefs regarding benevolence and integrity. We hypothesize:

Hypothesis H3b: Users' trust in other OSN members reduces their perceived privacy risk of disclosing on an OSN.

Perceived control

Even though trust can be an important means of risk-reduction, it does not enable people to actually control the behavior of others (Grabner-Kräuter and Kaluscha, 2003). Malhotra *et al*. (2004) view control as an active component of information privacy. Specifically, people tend to be less worried about data collection when they explicitly give permission to firms or are given the choice to opt-out (Novak and Phelps, 1995).

OSN providers can empower users with control by offering them granular privacy settings that enable them to limit access to their profile. In contrast, research findings show that many users regard privacy settings as insufficient (Boyd, 2008) or underutilize them because of their complexity (Strater and Richter, 2007). As a consequence, users tend to worry about potential negative outcomes: 'Everyone in my 500 plus friends' list knows how I feel and what I am doing or whatever I have in mind … but I want to share, maybe, with 20 people, but not with 500' (FG quotation).

Furthermore, users' willingness to control the use of their information can be addressed by OSNs' privacy policies. For example, Culnan (1995) demonstrates that people who know they can remove their names from marketing lists have fewer privacy concerns. Effective and transparent privacy statements on OSNs could offer users a frame of governance on how their information can be used by the provider and other parties. If policies granting users control are missing, privacy concerns may be magnified: 'it's a bit disturbing if I am not informed whether the information I provide is saved' (FG quotation). Xu *et al*. (2008) empirically demonstrate the importance of providing self-controlling mechanisms in order to diminish the perception of privacy risk on OSNs. Hence, we hypothesize:

Hypothesis H4a: Users' perceived control is negatively related to their perceived privacy risk on an OSN.

Research findings show that when companies grant consumers control over their information, consumers develop a more trusting attitude and are more willing to continue the relationship with the firm (Dinev and Hart, 2003). In the context of online interactions, empowering users with control is especially important, as the social distance between participants is significant (Culnan and Armstrong, 1999). Unsure about the incentives of the OSN providers, users may restrict their disclosures as the result of exaggerated risk perceptions exacerbated by the negative publicity of the OSN providers. Fair privacy policies and transparent, easy-to-use privacy controls may address this problem by signaling that an OSN provider can be trusted. For OSNs, these insights are important, as providers seek *operable* means to enhance their sites. Therefore, we hypothesize:

Hypothesis H4b: Users' perceived control is positively related to their trust in the OSN provider.

FG participants expressed a desire for more control with regard to other OSN members: 'On one hand I want as many people to see and to read about my thoughts … but on the other hand, you need some protection from them, and you have to find a balance yourself.' Das and Teng (1998) argue that control can be viewed as an important mechanism for creating confidence in cooperative behavior among participating parties. In this way, control helps to promulgate an atmosphere of trust on a platform. In fact, OSN users are likely to gain trust in other members when they are given clear tools for managing their privacy. These tools may include the ability to limit access to their profile, remove photo tags or comments and report improper behavior. Therefore, we hypothesize that:

Hypothesis H4c: Users' perceived control is positively related to their trust in other OSN members.

The summary of the model hypotheses is presented in Figure 1.

Empirical study

Survey design and sampling

An online questionnaire was distributed via numerous university mailing lists and postings in popular OSN

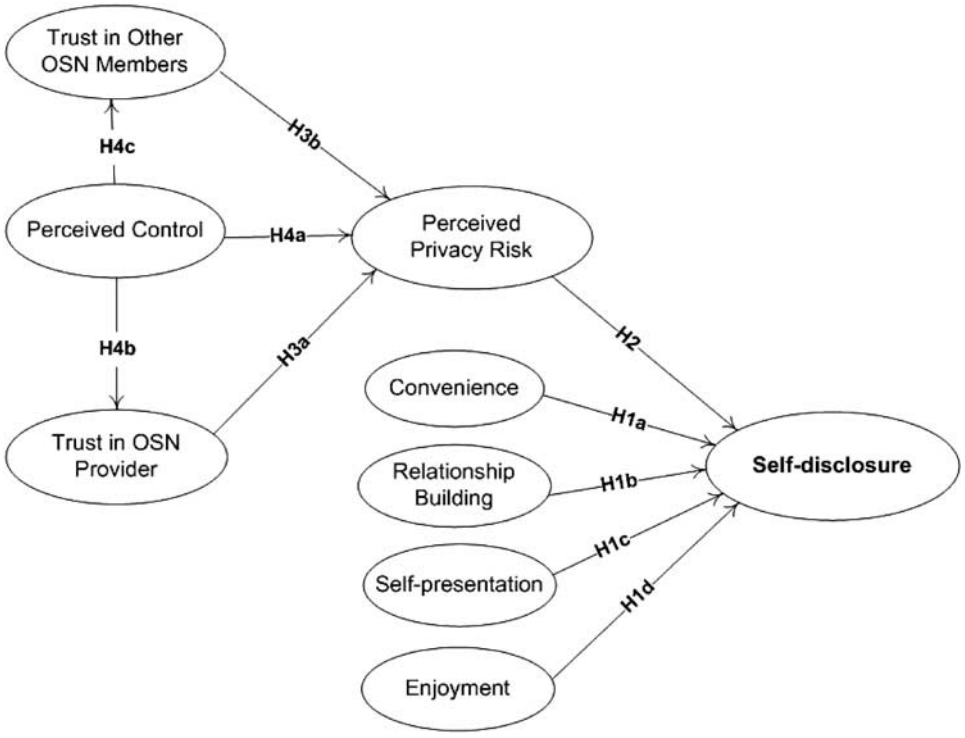

Figure 1 Research model of self-disclosure on online social networking sites.

groups. The survey targeted Facebook and StudiVZ users, two OSNs popular in Germany. In order to avoid the possible problem of a self-selection bias (e.g. OSN users more concerned about privacy might be more inclined to answer our privacy-related survey), we offered all participants to take part in a lottery of gift certificates. In doing so, we ensured that also users who were not particularly involved in OSNs responded to our survey.

The responses were collected from February to April 2008, with the overall gross sample consisting of 270 observations. After deleting observations that were unusable, a final net sample of 259 observations was obtained. Seventy percent of the respondents answered the survey for StudiVZ and 30% for Facebook. A total of 51.2% of the sample respondents were women; 85.8% were students; 86.2% were between 20 and 29 years old. Our sample, dominated by students, is representative of the user base of StudiVZ and also reflects an important group of Facebook users. Moreover in behavioral contexts, research suggests that results obtained on the basis of college samples are largely generalizable to the overall population, since diversity of attitudes in a society is also present among students (Kruglanski, 1975). Other characteristics of our sample largely correspond to the Facebook demographics: 56.2% of Facebook users are female, and over 60% are under 34 years old (insidefacebook.com, 2009).

Development of measurement scales

To test our hypotheses, we relied on pre-tested scales wherever possible. Nevertheless, most of the scales had to be modified to fit the OSN context. Particular attention was paid to the operationalization of the construct of self-disclosure: the self-developed items aimed to measure the amount of information a user provides in the process of participation on an OSN.

The Content Validity of the adapted and newly developed scales was ensured with the help of a structured sorting exercise (Moore and Benbasat, 1991) conducted with 10 volunteers. After a pre-test with 20 OSN users, several items with low inter-item correlations within a construct were eliminated. The full list of items included into a pre-test is available from authors upon request. The resulting list of items and their originating sources are presented in Table 2. Most of the items were measured on a seven-point Likert scale, with all constructs in the study modeled as being reflective.

Research methodology and results

We used Structural Equation Modeling to evaluate the research model presented in Figure 1. Theoretically, Structural Equation Modeling can be used for either theory testing and development (in which case the covariance-based approach is commonly applied) or for predictive application (which calls for the use of Partial Least Squares). However, as Anderson and Gerbing (1988: 411) put it, 'although it is convenient to distinguish between exploratory and confirmatory research, in practice this distinction is not as clear-cut.' Jöreskog (1974: 2) states that 'many investigations are to some extent both exploratory and confirmatory, since they involve some variables of known and other variables of unknown composition.' In this context, Jöreskog and Wold (1982: 270) argue that the covariance-based approach 'is theory-oriented, and emphasizes the transition from exploratory to confirmatory analysis.'

Given that our empirical study is primarily based on theory obtained from an extensive literature review, and

Table 2 Construct operationalization

Latent variable	*Item*	*Item text*
Convenience in relationship maintenance (self-developed; partly based on Chiu *et al*., 2006)	CON1	The OSN is convenient to inform all my friends about my ongoing activities
	CON2	The OSN allows me to save time when I want to share something new with my friends
	CON3	I find the OSN efficient in sharing information with my friends
Relationship building (self-developed)	RB1	Through the OSN I get connected to new people who share my interests
	RB2	The OSN helps me to expand my network
	RB3	I get to know new people through the OSN
Self-presentation (based on Walther *et al*., 2001)	SPR1	I try to make a good impression on others on the OSN
	SPR2	I try to present myself in a favorable way on the OSN
	SPR3[a]	The OSN helps me to present my best sides to others
Enjoyment (partly based on Nambisan and Baron, 2007)	EN1	When I am bored I often login to the OSN
	EN2	I find the OSN entertaining
	EN3	I spend enjoyable and relaxing time on the OSN
Perceived privacy risk (based on Malhotra *et al*., 2004)	RISK1	Overall, I see no real threat to my privacy due to my presence on the OSN (*Reversed*)
	RISK2[a]	I fear that something unpleasant can happen to me due to my presence on the OSN
	RISK3	I feel safe publishing my personal information on the OSN (*Reversed*)
	RISK4[a]	Overall, I find it risky to publish my personal information on the OSN
	RISK5	Please rate your overall perception of privacy risk involved when using the OSN (*very safe – very risky*)
Trust in OSN provider (based on McKnight *et al*., 2002a; Jarvenpaa and Tractinsky, 1999)		The OSN…
	TP1	… is open and receptive to the needs of its members
	TP2	… makes good-faith efforts to address most member concerns
	TP3	… is also interested in the well-being of its members, not just its own
	TP4	… is honest in its dealings with me
	TP5	… keeps its commitments to its members
	TP6[a]	… is trustworthy
Trust in other OSN members (based on Chiu *et al*., 2006; McKnight *et al*., 2002a)		Other members on the OSN …
	TM1[a]	… will do their best to help me
	TM2	… do care about the well-being of others
	TM3	… are open and receptive to the needs of each other
	TM4	… are honest in dealing with each other
	TM5[a]	… keep their promises
	TM6	… are trustworthy

Table 2 Continued

Latent variable	*Item*	*Item text*
Perceived control (self-developed)	PC1	I feel in control over the information I provide on the OSN
	PC2	Privacy settings allow me to have full control over the information I provide on the OSN
	PC3	I feel in control of who can view my information on the OSN
Self-disclosure (self-developed)	SD1	I have a comprehensive profile on the OSN
	SD2	I find time to keep my profile up-to-date
	SD3	I keep my friends updated about what is going on in my life through the OSN
	SD4	When I have something to say, I like to share it on the OSN

[a]removed during model fitting process (Confirmatory Factor Analysis).

that it incorporates relatively few exploratory elements from the FGs, we consider the covariance-based approach to be adequate. To account for both the new elements from the FGs and the fact that some of the measurement scales had to be adapted to the context of OSNs, we decided to run an Exploratory Factor Analysis (EFA) before analyzing the Measurement Model and Structural Model. Consequently, the evaluation of the research model in Figure 1 involved three stages: Explorative Factor Analysis of the items, Confirmatory Factor Analysis (CFA) of the Measurement Model and evaluation of the Structural Model (SM).

Explorative factor analysis

A principal components factor analysis with a Varimax rotation was performed on the collected data using SPSS 14.0 in order to check if the category structure present in our model was also reflected in the extracted factor groups. All indicators loaded strongly on the latent variables they were supposed to measure. Only four out of 37 items had loadings between 0.6 and 0.7, with the rest exceeding the level of 0.7. Additionally, all items but two fulfilled the narrow definition of 'factor purity' suggested by Saucier (1994: 509). Finally, the inter-item correlations for items of different constructs were, in absolute values, much smaller than those of items supposed to measure the same construct, thereby fulfilling Convergent and Discriminant Validity in concordance with classical EFA procedure (Homburg and Giering, 1996).

Analysis using Principal Axis Factoring as an alternative extraction method resulted in similar conclusions.

Data distribution

Multivariate normal distribution of data is an important pre-condition for the valid evaluation of the measurement and structural models (Byrne, 2001). Given that our data set exhibited a deviation from this assumption (skewness and kurtosis values for each variable are available from the authors upon request), we estimated our Measurement and Structural Models using the bootstrapping approach (BTSR) with 350 replications in addition to the traditional maximum likelihood (ML) analysis. A bias-corrected approach to interval estimation was chosen for both the Measurement Model and the Structural Model as recommended by Byrne (2001). The results between the maximum likelihood estimation and the bootstrapping approach differ only marginally so that the obtained results via maximum likelihood analysis are robust with respect to the non-normality of the data (Garson, 2009).

Measurement model – Confirmatory Factor Analysis

Building on the EFA results, in the next step we assessed reliability and validity of our model through a CFA with AMOS 16.0.1. In this analysis, all items were included and restricted to load on the respective construct they were supposed to measure. The constructs themselves were allowed to correlate with each other. In this process of model adjustment, several items were removed from the model as marked in Table 2. Taking into account the large number of newly developed scales, this practice is acceptable, as long as Content Validity remains fulfilled (Segars and Grover, 1993). All subsequent evaluations have been done with the adjusted model.

The Internal Consistency of the scales and Convergent Validity and Discriminant Validity of the measured constructs assessed on the basis of maximum likelihood analysis are shown in Tables 3 and 4. Internal Consistency is evaluated with Cronbach's Alpha, which for all constructs surpasses the recommended value of 0.7 (Nunnally, 1978). Thus, overall Internal Consistency can be assumed. Convergent Validity is assessed via three criteria. First, all indicator loadings are significant (*P*-values for significance were verified on the basis of maximum likelihood and bootstrap bias-corrected confidence intervals) and exceed the level of 0.5 (Bagozzi and Yi, 1988; Hair *et al*., 1998). Second, it is more important that the indicators together measure their respective construct well (Bagozzi and Baumgartner, 1994). This can be evaluated by the Composite Reliability. All values greatly surpass the minimum required threshold of 0.6 (Bagozzi and Yi, 1988), ensuring Composite Reliability. Finally, as the third criterion, the Average Variance Extracted (AVE) of the constructs should lie above 0.5 to ensure that the variance explained by the construct is larger than the variance due to measurement error (Fornell and Larcker, 1981). This

Table 3 Quality criteria of the constructs

Latent variable	*Item*	*Mean*	*Standard deviation*	*Standardized factor loading*	*AVE*	*Composite reliability*	*Cronbach's alpha*
Convenience in relationship maintenance	CON1	4.19	1.78	0.730	0.61	0.82	0.82
	CON2	4.23	1.77	0.770			
	CON3	4.57	1.71	0.833			
Relationship building	RB1	3.79	1.77	0.662	0.43	0.69	0.70
	RB2	4.16	1.73	0.734			
	RB3	2.99	1.71	0.569			
Self-presentation	SPR1	3.84	1.69	0.877	0.75	0.85	0.86
	SPR2	4.16	1.62	0.851			
Enjoyment	EN1	4.73	1.70	0.578	0.50	0.75	0.74
	EN2	5.14	1.30	0.652			
	EN3	4.56	1.41	0.869			
Perceived privacy risk	RISK1	4.24	1.79	0.703	0.60	0.82	0.80
	RISK3[a]	4.03	1.26	0.779			
	RISK5	4.05	1.17	0.838			
Trust in OSN provider	TP1	3.67	1.36	0.707	0.56	0.86	0.87
	TP2	3.83	1.24	0.720			
	TP3	4.05	1.23	0.747			
	TP4	3.69	0.94	0.775			
	TP5	3.67	0.96	0.793			
Trust in other OSN members	TM2	3.61	1.00	0.851	0.68	0.9	0.90
	TM3	3.50	0.99	0.830			
	TM4	4.30	1.78	0.843			
	TM6	3.83	1.64	0.782			
Perceived control	PC1	4.25	1.71	0.725	0.54	0.78	0.77
	PC2	3.32	1.74	0.829			
	PC3	3.28	1.71	0.633			
Self-disclosure	SD1	3.23	1.79	0.622	0.51	0.81	0.80
	SD2	3.08	1.59	0.739			
	SD3	2.77	1.60	0.775			
	SD4	2.62	1.56	0.715			

[a]responses for RISK3 have been reversed prior to evaluation.

criterion is fulfilled for all of our constructs with the exception of Relationship Building. In order to capture well all facets of this heterogeneous construct and to preserve its Content Validity established in the structured sorting process, it was however not possible to remove any of the indicators of Relationship Building. Additionally, the results of the EFA hinted to a good Convergent Validity of the Measurement Model. Overall, from these facts we conclude that Convergent Validity is fulfilled.

Table 4 can be used to evaluate Discriminant Validity. For each latent variable, the square root of AVE (diagonal element) is larger than the absolute value of the correlation between this latent variable and any other latent variable (absolute values of off-diagonal elements) (Fornell and Larcker, 1981). Additionally, the standardized cross-factor loadings are much smaller than the loadings of the indicators on their own constructs (table available from the authors upon request). As a result, we can assume that there is Discriminant Validity.

To further assess the quality of the model, overall measures of goodness-of-fit can be computed (see Table 5, column 'CFA'). Given that the Chi-square (χ^2) test is highly sensitive to the deviations in data distribution, a Bollen-Stine bootstrap approach was chosen to evaluate the null hypothesis that the model we specified was correct (Byrne, 2001). The bootstrapping procedure rendered a *P*-value of 0.251, which clearly leads us to conclude that our Measurement Model has an adequate fit.

In the next step, more traditional measures of goodness-of-fit were evaluated. The Goodness-of-Fit Index (GFI)

Table 4 Square root of average variance extracted (diagonal elements) and correlation between latent variables (off-diagonal elements)

	CON	*RB*	*SPR*	*EN*	*RI*	*TP*	*TM*	*PC*	*SD*
Convenience (CON)	*0.781*								
Relationship building (RB)	0.242	*0.656*							
Self-presentation (SPR)	0.161	0.216	*0.866*						
Enjoyment (EN)	0.440	0.272	0.370	*0.707*					
Perceived privacy risk (RI)	−0.213	0.013	−0.285	−0.367	*0.775*				
Trust in OSN provider (TP)	0.385	0.257	0.186	0.383	−0.602	*0.748*			
Trust in other OSN members (TM)	0.092	0.009	0.146	0.037	−0.150	0.184	*0.825*		
Perceived control (PC)	0.320	0.058	0.168	0.289	−0.657	0.623	0.188	*0.735*	
Self-disclosure (SD)	0.557	0.303	0.239	0.495	−0.417	0.480	0.231	0.405	*0.714*

Table 5 Goodness-of-fit measures for confirmatory factor analysis and structural model

Goodness-of-fit measure	*Recommended cut-off criterion (source)*	*CFA*	*SM*
P-value for the χ^2-test according to Bollen-Stine bootstrap	>0.05 (significance level of 5%) (Byrne, 2001)	0.251	0.125
GFI	>0.90 (Jöreskog and Sörborm, 1989) >0.80 (Etezadi-Amolo and Farhoomand, 1996)	0.895	0.884
AGFI	>0.80 (Jöreskog and Sörborm, 1989)	0.867	0.860
RMSEA	<0.06 (Hu and Bentler, 1999)	0.032	0.037
Hoelter's Critical *N* at 0.01	$<$Sample size $N=259$ (Hoelter, 1983)	240	226
CFI	>0.95 (Hu and Bentler, 1999)	0.970	0.960
IFI	>0.95 (Hu and Bentler, 1999)	0.971	0.961
TLI	>0.95 (Hu and Bentler, 1999)	0.965	0.955

amounts to 0.895, which exceeds the recommended threshold of 0.80 (Etezadi-Amolo and Farhoomand, 1996), and is only slightly smaller than the narrower cut-off criterion of 0.90 (Jöreskog and Sörborm, 1989). The Adjusted GFI (AGFI) exceeds the required value of 0.80 (Jöreskog and Sörborm, 1989). However, it has to be stressed that the performance of these measures of the overall fit has been put into question in the recent literature on Structural Equation Modeling. In particular, Hu and Bentler (1998, 1999) discourage from using these indices for model evaluation. Today, researchers typically prefer to evaluate the Root Mean Square Error of Approximation (RMSEA) which should be smaller than 0.06 for a good model fit (Hu and Bentler, 1999). This criterion is met by our model with an RMSEA of 0.032. Also note that the sample size exceeds Hoelter's 'Critical N' (CN), which is 'the size that a sample must reach in order to accept the fit of a given model on a statistical basis' (Hoelter, 1983: 330). In addition to these absolute fit indices, we also computed incremental ones. To be specific, the Comparative Fit Index (CFI), the Incremental Fit Index (IFI) as well as the Tucker-Lewis Index (TLI) exceed the cut-off threshold of 0.95 suggested by Hu and Bentler (1999), with respective values of 0.970, 0.971 and 0.965, in our model. All in all, these results suggest that our Measurement Model is well specified.

Structural model

We now turn to the evaluation of the Structural Model, reporting the corresponding quality criteria in Table 5, column 'SM.' Again, our Structural Model meets all cut-off criteria. Following the same line of arguments as for the Measurement Model, we conclude that the Structural Model has a good overall fit.

Table 6 presents the results of the hypothesis evaluation: the standardized path coefficients together with the corresponding *P*-values on their significance estimated on the basis of maximum likelihood and the bootstrapping approach. As mentioned above, even though the estimation via the bootstrapping approach rendered slightly higher estimates for the *P*-values of several respective path coefficients, the outcome of the estimation (the significance or insignificance of the estimated path coefficients) remained the same. Figure 2 graphically summarizes the results obtained on the basis of the maximum likelihood analysis.

Table 6 Standardized path coefficients, *P*-values and hypothesis evaluation

Hypothesis	*Construct A → Construct B*	*Path coefficient*	*P-value ML*	*P-value BTSR*	*Rejected/ supported*
H1a	Convenience → Self-disclosure	0.377	0.000***	0.005**	Supported
H1b	Relationship building → Self-disclosure	0.155	0.037*	0.033*	Supported
H1c	Self-presentation → Self-disclosure	0.006	0.930	0.996	Rejected
H1d	Enjoyment → Self-disclosure	0.194	0.019*	0.037*	Supported
H2	Perceived privacy risk → Self-disclosure	−0.277	0.000***	0.010**	Supported
H3a	Trust in OSN provider → Perceived privacy risk	−0.288	0.002**	0.013*	Supported
H3b	Trust in other OSN members → Perceived privacy risk	−0.010	0.863	0.938	Rejected
H4a	Perceived control → Perceived privacy risk	−0.488	0.000***	0.005**	Supported
H4b	Perceived control → Trust in OSN provider	0.655	0.000***	0.010**	Supported
H4c	Perceived control → Trust in other OSN members	0.205	0.005**	0.023*	Supported

*Significance at 5%, **Significance at 1%, ***Significance at 0.1%.

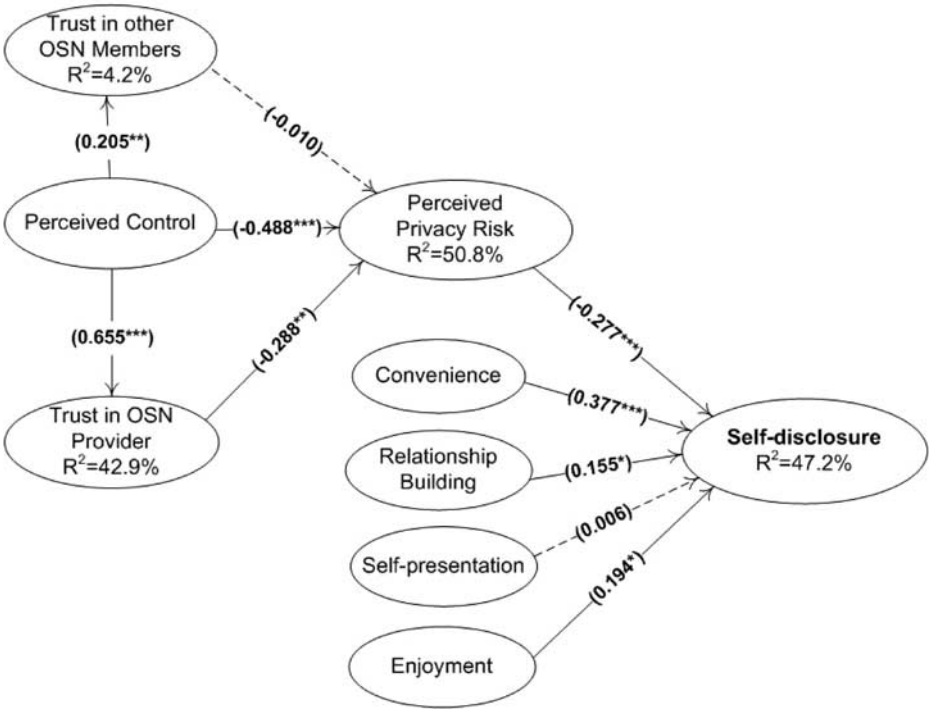

Figure 2 Results of the structural model. *Significance at 5%, **Significance at 1%, ***Significance at 0.1%. ——— represents a significant link; - - - - - - represents an insignificant link.

Finally, our model explains $R^2 = 47.2\%$ of the variance in our main dependent latent variable – self-disclosure. This value exceeds the required cut-off criterion of 0.4 (Homburg and Baumgartner, 1995) and indicates a high explanatory power of the model. Nevertheless, we recognize that other factors beyond those investigated in our study, such as peer pressure (Acquisti and Gross, 2006), perceived anonymity (Joinson and Paine, 2007) or anticipation of face-to-face encounter (Gibbs *et al*., 2006) can also impact individual self-disclosure and, hence, enhance the explanatory power of the model.

The implications of the obtained results are discussed in the following sections.

Discussion of results and managerial implications

Benefits as motivators of self-disclosure on OSNs

In this study, we have examined several gratification mechanisms with regard to individual self-disclosure on OSNs. We find that the Convenience of Maintaining Relationships is an important determinant of Self-disclosure. Convenience benefits arise as a result of the OSN design, which places users just 'one click away' from each other and allows them to easily and efficiently update a large group of friends and acquaintances. A small post on the wall is a simple way to remind others about oneself, helping to keep

relationships alive. Additionally, we confirm that people looking for new friendships – Relationship Building benefits – disclose more about themselves in their attempt to find common ground with unknown people. Furthermore, we find Enjoyment to be a significant driver of self-disclosure. Indeed, new features that address users' pleasure motive are continuously integrated into the platforms, encouraging users to reveal more information and creating site stickiness.

To our surprise, we find no link between self-presentation benefits and self-disclosure in OSNs. One explanation for this phenomenon may be that participants do not need to disclose a lot of information to project a certain image of themselves. Furthermore, at the current maturity stage of the OSNs, tight interdependence of friends with each other may lead users to realize that exaggerated self-enhancement can be easily recognized by others. Additionally, despite strict reliance on the pre-tested measurement scales, the self-presentation construct is particularly susceptible to the social desirability bias. When asked directly, people rarely say that they aim to present themselves in a better light. Even without the direct link, a quick look at Table 4 reveals that self-presentation has the highest correlation with the Enjoyment construct (correlation coefficient is 0.370); this suggests some incremental pleasure of self-presentation. In fact, Social Psychology theories treat pleasure as a by-product or consequence of satiating motives (Reiss, 2004).

Overall, our findings suggest that OSNs are becoming attractive easy-to-use functional tools, similar to enhanced address-books, rather than impression management platforms.

Risk perceptions of disclosure on OSNs

As expected, perceived privacy risk has a significant negative impact on the amount of information disclosed. Users adjust how much information they disclose based on the privacy threats they perceive. However, the impact of perceived privacy risk on self-disclosure is lower than that of the benefits (the corresponding *t*-test yielded a test-statistic of 2.805). This result reveals that the rewards people gain from engaging in intensive communication on OSNs can overshadow the risks and induce them to reveal more information.

This is partly due to mitigating factors, which reduce users' perception of risk with regard to information disclosure: Perceived control and trust in the OSN provider. Thus, functional features, such as privacy settings and clear information on privacy-related procedures may be significant means of reducing the privacy risk. Furthermore, our results show that the feeling of being in control enhances the user trust in the OSN provider. By providing the right spectrum of functional controls OSN providers thus have a means to ensure users' trust in the network provider and indirectly encourage communication. In a similar fashion, available control options, such as the ability to limit one's profile or report other users, give users the feeling of being protected and therefore increase trust within the community.

Interestingly, we find that trust in other OSN members failed to alleviate privacy risks in any meaningful way. This finding suggests that user privacy concerns mainly center on organizational risks such as collection and secondary use of their information. Users may believe companies have more incentive to abuse their information compared to other network members.

Implications for OSN providers

Despite the unprecedented growth rates of OSNs, current statistics show that OSN users gradually start to lose interest and become less active (Schmidt, 2008). In the light of these developments, the results of our study have a lot of implications for OSN providers.

From a motivational perspective, our results indicate that OSNs should have an even stronger interest in enriching their core functionality: facilitating the maintenance of relationships (e.g. birthday reminders, reflection of relationship hierarchies). Furthermore, providers should foster relationship building among participants by actively presenting them to each other (e.g. by listing users currently online by category). Additionally, network providers should place more emphasis on the enjoyment aspect by bringing their functionality to a level of immersion equal to virtual world communities. They could, for example, introduce collaborative online games.

On the negative side, OSN providers should be aware that perceived privacy risks do prevent self-disclosure. Our study reveals two key mechanisms involved in the mitigation of risk concerns: improving user control and increasing trust in the OSN provider.

The importance of perceived control indicates that, when it comes to user options, OSN providers cannot afford to force privacy into the background. If OSN providers make privacy management more transparent, consistent and user-friendly, users will perceive a much lower degree of risk. Providers can further strengthen users' perception of behavioral control by giving users choices over how their data are accessed and giving them visual feedback confirming the effectiveness of their decisions. Additionally, providers can empower users by pro-actively informing them about what is being done with their data and providing simple lists of rules (instead of overwhelming legal texts). In contrast, most users today are still unsure of whether their information is really deleted once they close their account.

To enhance trust, OSN providers must continue to implement fair privacy policies and offer transparent and clear-cut procedures for dealing with privacy abuse. Importantly, providers should prevent information collection by third parties and protect the OSN site from unauthorized access by online crawlers. To ensure network sustainability, providers can also utilize advertising campaigns supporting the reputation of the OSN provider as a trustworthy entity. Most importantly, the OSN provider must behave in a consistent and fair manner with its users.

Conclusion

Inspired by rising privacy concerns, our study empirically identifies factors involved in self-disclosure on OSNs. We find that among the myriad benefits of OSN platforms, Convenience, Relationship Building and Enjoyment are significantly linked to information disclosure. We contribute to

the ongoing research by showing that, although risk hinders self-disclosure, it is often offset by benefits and mitigated by trust and control beliefs. Our findings demonstrate that OSN members engage in a process of privacy calculus when deciding to disclose information. From a practical perspective, our results provide important insights for OSN providers by identifying areas where they should invest resources in order to ensure more communication and user activity on the network.

Looking at individual self-disclosure primarily through a privacy calculus lens, we recognize that other factors beyond those investigated in our study can also have an impact on individual self-disclosure. However, we did not include these constructs into our model – a potential shortcoming of our approach and a venue for future research. Furthermore, considering that most of our survey respondents were students, our model can still be validated with a more global population of OSN users.

References

Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, information sharing, and privacy on the facebook, in 6th Workshop on Privacy Enhancing Technologies (Cambridge, UK, 2006); Berlin: Springer-Verlag, 36-58.

Anderson, J.C. and Gerbing, D.W. (1988). Structural Equation Modeling in Practice: A review and recommended two-step approach, *Psychological Bulletin* **103**(3): 411–423.

Bagozzi, R.P. and Baumgartner, H. (1994). The Evaluation of Structural Equation Models and Hypothesis Testing, in R.P. Bagozzi (ed.) *Principles of Marketing Research*, Cambridge: Blackwell, pp. 386–422.

Bagozzi, R.P. and Yi, Y. (1988). On the Evaluation of Structural Equation Models, *Journal of the Academy of Marketing Science* **16**(1): 74–94.

Boyd, D. (2007). Why Youth (Heart) Social Network Sites: The role of networked publics in teenage social life, in D. Buckingham (ed.) *Youth, Identity, and Digital Media*, Cambridge: MIT Press, pp. 119–142.

Boyd, D. (2008). Facebook's Privacy Trainwreck: Exposure, invasion and social convergence, *Convergence* **14**(1): 13–20.

Byrne, B.M. (2001). *Structural Equation Modeling with AMOS: Basic concepts, applications and programming*, USA: Lawrence Erlbaum Associates.

Chiu, C.-M., Hsu, M-H. and Wang, E.T.G. (2006). Understanding Knowledge Sharing in Virtual Communities: An integration of social capital and social cognitive theories, *Decision Support Systems* **42**(3): 1872–1888.

Chopra, K. and Wallace, W.A. (2003). Trust in Electronic Environments, in 36th Annual Hawaii Conference on System Sciences (Big Island, USA, 2003); Chicago: IEEE Computer Society Press, Track 9, Vol. 9.

Culnan, M.J. (1995). Consumer Awareness of Name Removal Procedures: Implications for direct marketing, *Journal of Direct Marketing* **9**(2): 10–19.

Culnan, M.J. and Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An empirical investigation, *Organization Science* **10**(1): 104.

Das, T.K. and Teng, B. (1998). Between Trust and Control: Developing confidence in partner cooperation in alliances, *Academy of Management Review* **23**(3): 491–512.

Dinev, T. and Hart, P. (2003). Privacy Concerns and Internet Use – A model of trade-off factors, in Academy of Management Meeting (Seattle, USA, 2003) [www document] http://www.ebusinessforum.gr/old/content/downloads/Privacy%20Concerns%20And%20Internet%20Use%20_A%20Model%20Of%20Trade-Off%20Factors.pdf (accessed 28th October 2009).

Dinev, T. and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research* **17**(1): 61–80.

Dwyer, C., Hiltz, S.R. and Passerini, K. (2007). Trust and Privacy Concern within Social Networking Sites: A comparison of facebook and myspace, in Americas Conference on Information Systems (Keystone, USA, 2007), [www document] http://aisel.aisnet.org/amcis2007/339 (accessed 28th October 2009). Paper 339.

Ellison, N., Heino, R. and Gibbs, J. (2006). Managing Impressions Online: Self-presentation processes in the online dating environment, *Journal of Computer-Mediated Communication* **11**(2), [www document] http://jcmc.indiana.edu/vol11/issue2/ellison.html (accessed 28th October 2009).

Ellison, N.B., Steinfield, C. and Lampe, C. (2007). The Benefits of Facebook "Friends" Social capital and college students' use of online social network sites, *Journal of Computer-Mediated Communication* **12**(4), [www document] http://jcmc.indiana.edu/vol12/issue4/ellison.html (accessed 28th October 2009).

Etezadi-Amolo, J. and Farhoomand, A.F. (1996). A Structural Model of end User Computing Satisfaction and User Performance, *Information and Management* **30**(2): 65–73.

Facebook.com (2009). Statistics, Press Center [www document] http://www.facebook.com/press/info.php?statistics (accessed 28th October 2009).

Feng, J., Lazar, J. and Preece, J. (2004). Empathy and Online Interpersonal Trust: A fragile relationship, *Behavior & IT* **23**(2): 97–106.

Fornell, C. and Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research* **18**(3): 39–50.

Garson, G.D. (2009). Structural Equation Modeling, Statnotes: Topics in multivariate analysis, (last updated on 10th August 2009) [www document] http://faculty.chass.ncsu.edu/garson/PA765/structur.htm#amosboot (accessed 28th October 2009).

Gefen, D., Rao, V.S. and Tractinsky, N. (2003). The Conceptualization of Trust, Risk, and their Relationship in Electronic Commerce: The need for clarifications, in 36th Hawaii International Conference on System Sciences (Big Island, USA, 2003); Chicago: IEEE Computer Society Press, 192–201.

Gibbs, J.L., Ellison, N.B. and Heino, R.D. (2006). Self-Presentation in Online Personals, *Communication Research* **33**(2): 152–177.

Grabner-Kräuter, S. and Kaluscha, E.A. (2003). Empirical Research in On-line Trust: A review and critical assessment, *International Journal of Human-Computer Studies* **58**(6): 783–812.

Gross, R. and Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks, in ACM Workshop on Privacy in the Electronic Society (Alexandria, VA, USA, 2005); New York, NY, USA: ACM, 71–80.

Hair, J.F., Anderson, R.E., Tatham, R.L. and Black, W.C. (1998). *Multivariate Data Analysis with Readings*, 5th edn, Englewood Cliffs: Prentice-Hall.

Hann, I.-H., Hui, K.L., Lee, S.-Y.T. and Png, I.P.L. (2007). Overcoming Information Privacy Concerns: An information processing theory approach, *Journal of Management Information Systems* **24**(2): 13–42.

Hoelter, J.W. (1983). The Analysis of Covariance Structures: Goodness-of-fit indices, *Sociological Methods & Research* **11**: 325–344.

Hogben, G. (2007). Security Issues and Recommendations for Online Social Networks, ENISA Position Paper No. 1 [www document] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf (accessed 28th October 2009).

Homans, G.C. (1958). Social Behavior as Exchange, *American Journal of Sociology* **63**: 597–606.

Homburg, C. and Baumgartner, H. (1995). Beurteilung von Kausalmodellen – Bestandsaufnahme und Anwendungsempfehlungen, *Marketing Zeitschrift für Forschung und Praxis* **17**(3): 162–176.

Homburg, C. and Giering, A. (1996). Konzeptualisierung und Operationalisierung komplexer Konstrukte, *Marketing – Zeitschrift für Forschung und Praxis* **18**(1): 5–24.

Hu, L. and Bentler, P.M. (1998). Fit Indices in Covariance Structure Modeling: Sensitivity to underparameterized model misspecification, *Psychological Methods* **3**: 424–453.

Hu, L. and Bentler, P.M. (1999). Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling* **6**(1): 1–55.

Hui, K.-L., Tan, B.C.Y. and Goh, C.-Y. (2006). Online Information Disclosure: Motivators and measurements, *ACM Transactions on Internet Technology* **6**(4): 415–441.

insidefacebook.com (2009). Fastest Growing Demographic on Facebook: Women over 55, [www document] http://www.insidefacebook.com/2009/02/02/fastest-growing-demographic-on-facebook-women-over-55/ (accessed 28th October 2009).

Jarvenpaa, S.L. and Tractinsky, N. (1999). Consumer Trust in an Internet Store: A cross-cultural validation, *Journal of Computer-Mediated Communication* **5**(2), [www document] http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html (accessed 28th October 2009).

Joinson, A.N. and Paine, C.B. (2007). Self-Disclosure, Privacy and the Internet, in A.N. Joinson, K. McKenna, T. Postmes and U. Reips (eds.) *Oxford*

Handbook of Internet Psychology, Oxford: Oxford University Press, pp. 237–252.

Jöreskog, K.G. (1974). Analyzing Psychological Data by Structural Analysis of Covariance Matrices, in D.H. Krantz, R.C. Atkinson, R.D. Luce and P. Suppes (eds.) *Contemporary Developments in Mathematical Psychology*, Vol. 2, San Francisco: Freeman, pp. 1–56.

Jöreskog, K.G. and Sörborm, D. (1989). *LISREL-7 User's Reference Guide*, Mooresville: Scientific Software.

Jöreskog, K.G. and Wold, H. (1982). The ML and PLS Techniques for Modeling with Latent Variables: Historical and comparative aspects, in H. Wold and K. Jöreskog (eds.) *Systems Under Indirect Observation: Causality, structure, prediction*, Vol. 1, Amsterdam: North-Holland, pp. 263–270.

Kim, D.J., Ferrin, D.L. and Rao, R.H. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The role of trust, perceived risk, and their antecedents, *Decision Support Systems* **44**(2): 544–564.

Krasnova, H., Hildebrand, T., Günther, O., Kovrigin, S. and Nowobilska, A. (2008). Why Participate in an Online Social Networks: An empirical analysis, in W. Golden, T. Acton, K. Conboy, H. van der Heijden and V.K. Tuunainen, (eds.) Proceedings of 16th European Conference on Information Systems (Galway, Ireland; 2008), 2124–2135.

Krasnova, H., Kolesnikova, E. and Günther, O. (2009). It Won't Happen To Me!: Self-Disclosure in Online Social Networks, in Americas Conference on Information Systems (San Francisco, USA, 2009), [www document] http://aisel.aisnet.org/amcis2009/343 (accessed 28th October 2009). Paper 343.

Kruglanski, A.W. (1975). The Human Subject in the Psychology Experiment: Fact and artifact, in L. Berkowitz, (ed.) *Advances in Experimental Social Psychology*, Vol. 8, New York: Academic Press, pp. 101–147.

Lampe, C., Ellison, N. and Steinfield, C. (2007). A Familiar Face(book): Profile elements as signals in an online social network, in SIGCHI Conference on Human Factors in Computing Systems (San Jose, USA, 2007); New York: ACM, 435-444.

Landis, J.R. and Koch, G.G. (1977). The Measurement of Observer Agreement for Categorical Data, *Biometrics* **33**(1): 159–174.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model, *Information Systems Research* **15**(4): 336–355.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995). An Integrative Model of Organizational Trust, *Academy of Management Review* **20**(3): 709–734.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002a). Developing and Validating Trust Measures for E-commerce: An integrative typology, *Information Systems Research* **13**(3): 334–359.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002b). The Impact of Initial Consumer Trust on Intentions to Transact with a Web site: A trust building model, *Journal of Strategic Information Systems* **11**: 297–323.

Metzger, M.J. (2004). Privacy, Trust, and Disclosure: Exploring barriers to electronic commerce, *Journal of Computer-Mediated Communication* **9**(4), [www document] http://jcmc.indiana.edu/vol9/issue4/metzger.html (accessed 28th October 2009).

Moore, G.C. and Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation, *Information Systems Research* **2**(2): 192–222.

Muniz, A. and O'Guinn, T. (2001). Brand Community, *Journal of Consumer Research* **27**: 412–432.

Nambisan, S. and Baron, R.A. (2007). Interactions in Virtual Customer Environments: Implications for product support and customer relationship management, *Journal of Interactive Marketing* **21**(2): 42–62.

Novak, G.J. and Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and when 'privacy' matters, *Journal of Direct Marketing* **9**(3): 46–60.

Nunnally, J.C. (1978). *Psychometric Theory*, 2nd edn, New York: McGraw-Hill.

Pavlou, P.A. (2003). Consumer Acceptance of Electronic Commerce: Integrating trust and risk with the technology acceptance model, *International Journal of Electronic Commerce* **7**(3): 101–134.

Reiss, S. (2004). Multifaceted Nature of Intrinsic Motivation: The theory of 16 basic desires, *Review of General Psychology* **8**(3): 179–193.

Ridings, C., Gefen, D. and Arinze, B. (2002). Some Antecedents and Effects of Trust in Virtual Communities, *Journal of Strategic Information Systems* **11**(3-4): 271–295.

Rizk, R., Marx, D., Schrepfer, M., Zimmermann, J. and Günther, O. (2009). Media Coverage of Online Social Network Privacy Issues in Germany – A thematic analysis, in Americas Conference on Information Systems (San Francisco, USA, 2009), [www document] http://aisel.aisnet.org/amcis2009/342 (accessed 28th October 2009). Paper 342.

Rosen, P. and Sherman, P. (2006). Hedonic Information Systems: Acceptance of social networking websites, in Americas Conference on Information Systems (Acapulco, Mexico, 2006), [www document] http://works.bepress.com/peterrosen/2 (accessed 28th October 2009). Paper 162.

Ryan, G.W. and Bernard, H.R. (2000). Data Management and Analysis Methods, in N. Denzin and Y. Lincoln (eds.) *Handbook of Qualitative Research*, 2nd edn, Thousand Oaks, CA: Sage, pp. 769–802.

Saucier, G. (1994). Mini-Markers: A brief version of Goldberg's unipolar Big-Five markers, *Journal of Personality Assessment* **63**(3): 506–516.

Schmidt, H. (2008). Verweildauer in sozialen Netzwerken sinkt, in Frankfurter Allgemeine Zeitung 59 [www document] http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EF2AB62A5295040F3B76B3AF37BC4187E~ATpl~Ecommon~Scontent.html (accessed 28th October 2009).

Segars, A.H. and Grover, V. (1993). Re-Examining Perceived Ease of Use and Usefulness: A confirmatory factor analysis, *MIS Quarterly* **17**(4): 517–525.

Skinner, E.A. (1996). A Guide to Constructs of Control, *Journal of Personality and Social Psychology* **71**(3): 549–570.

Sledgianowski, D. and Kulviwat, S. (2008). Social Network Sites: Antecedents of user adoption and usage, in Americas Conference on Information Systems (Toronto, Canada, 2008), [www document] http://aisel.aisnet.org/amcis2008/83 (accessed 28th October 2009). Paper 83.

Son, J.-Y. and Kim, S.S. (2008). Internet Users' Information Privacy-Protective Responses: A taxonomy and a nomological model, *MIS Quarterly* **32**(3): 503–529.

Strater, K. and Richter, H. (2007). Examining Privacy and Disclosure in a Social Networking Community, in Symposium on Usable Privacy and Security (Pittsburgh, USA, 2007), New York, NY, USA: ACM, 157–158.

Stutzman, F. (2006). An Evaluation of Identity-Sharing Behavior in Social Network Communities, *International Digital and Media Arts Journal* **3**(1): 10–18.

Walczuch, R. and Lundgren, H. (2004). Psychological Antecedents of Institution-Based Consumer Trust in e-Retailing, *Information and Management* **42**(1): 159–177.

Walther, J.B. (1996). Computer-Mediated Communication: Impersonal, interpersonal, and hyperpersonal interaction, *Communication Research* **23**(1): 3–44.

Walther, J.B., Slovacek, C.L. and Tidwell, L.C. (2001). Is a Picture Worth a Thousand Words? Photographic Images in Long-term and Short-term Computer-mediated Communication, *Communication Research* **28**(1): 105–134.

Wheeless, L.R. and Grotz, J. (1976). Conceptualization and Measurement of Reported Self-disclosure, *Human Communication Research* **2**(4): 338–346.

Wieschowski, S. (2007). Studenten demonstrieren gegen das SchnüffelVZ, [www document] http://www.spiegel.de/netzwelt/web/0,1518,523906,00.html (accessed 28th October 2009).

Xu, X., Dinev, T., Smith, H.J. and Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an integrative view, in International Conference on Information Systems (Paris, France, 2008), [www document] http://aisel.aisnet.org/icis2008/6 (accessed 28th October 2009). Paper 6.

About the authors

Hanna Krasnova is a post-doctoral researcher at the Institute of Information Systems, School of Business and Economics, Humboldt-Universität zu Berlin. Before joining the institute in 2006, Hanna graduated with honors from the Belarusian State Economic University specializing in International Economic Relations in 2002. In 2006 she graduated as a Master of Arts in Economics and Management Science from the Humboldt-Universität zu Berlin, where she also received her doctoral degree in 2009. Hanna was a scholarship holder from DAAD and FSA ACCELS programs. Her primary research interests include aspects of

human-computer interaction in the area of online social networks.

Sarah Spiekermann is Chair of the Institute for Management Information Systems Vienna University of Economics and Business (WU Wien) and Adjunct Professor at the Heinz College of Public Policy and Management, Carnegie Mellon University (Pittsburgh, USA). Her research focus is value sensitive and behaviorally informed system design. Before she joined academia in 2003, she worked as a business consultant for A.T. Kearney and led the European business intelligence for Openwave Systems.

Ksenia Koroleva is a research assistant at the Institute of Information Systems, School of Business and Economics, Humboldt-Universität zu Berlin. She received her Master of Science degree in Economics and Management at the Humboldt-University with majors in Finance and Information Systems in 2008, as well as Diploma in Management with distinction from the University for Engineering and Economics in St. Petersburg in 2005. During her studies she was a scholarship holder from DAAD, Friedrich-Naumann-Stiftung and FSA ACCELS program. Her research interests include value and acceptance of IT, ranging from Wireless Applications to Social Networking.

Thomas Hildebrand joined the European School of Management and Technology (ESMT) as a research assistant in 2006 after graduating in Economics from Humboldt-Universität zu Berlin. During his studies he participated in the integrated double-diploma program of Humboldt-Universität and the Ecole Nationale de la Statistique et de l'Administration Economique (ENSAE) in France, receiving additionally the diploma of a Statisticien-Economiste. During several internships Thomas worked for Ernst & Young and the Federal Treasury Ministry. Thomas's research interests are in the areas of Microeconomics (in particular Network Externalities and Two-Sided Markets), Financial Intermediation and Social Networks.